REMARKS

The Office Action dated August 16, 2005 has been reviewed and carefully considered. Claim 30 is added. <u>No claims are amended</u>. Claims 1-30 are pending in the application, of which the independent claims remain 1, 2, 8, 13 and 18. Reconsideration of the above-identified application, as amended and in view of the following remarks, is respectfully requested.

Claims 1-29 stand rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent No. 5,799,081 to Kim et al. ("Kim") in view of U.S. Patent No. 6,550,008 to Zhang et al. ("Zhang") and ITU-T Recommendation H.222.0 (hereinafter "ITU-T").

Claim 1 recites:

> point of deployment module generates a reply message which <u>includes at least one control information pair</u>, relating to the information, <u>each control information pair having copy control information</u> and a stream identifier . . . respectively <u>generating</u> a first key in the point of deployment module and a second key in the set-top box, <u>using the at least one control information pair</u>

Firstly, the Office Action seems to select the Kim copy protection control signal CP from the smart card 261 to the integrated receiver/decoder (or "set-top box") 266 as the "copy control information" of the present claim 1, but does not explain what would supposedly would have served as motivation for the Kim/Zhang/ITU-T combination the Office Action proposes.

The selection, by the Office Action, of Kim signal CP appears to suggest the Office Action regards this signal as the Zhang binding information that Zhang sends from the POD to the host.

The Office Action seems to relocate at least the Kim controller 262 to the smart card 261. Presumably, then, the incoming bitstream is rerouted to the card, and comes back to the host augmented with the CP signal.

However, firstly, Zhang sends the binding information to the host only so that the host will be able to generate a shared key for safe traversal of the interface between the host and the POD. Zhang does not send the binding information to the host for other functions such as copy control. It is accordingly unclear where, from the references and what was generally known to those of ordinary skill in the art, would have arisen the idea of using payload in generating a one-way hash across an a POD/host interface. Perhaps, the Examiner contemplates the IS-POD-CP document (instant specification, page 10, line 9. However, that document has a publication date of October 27, 1999 (page 10, line 9), which comes after the effective filing date of the present application (see preliminary amendment, first page).

Secondly, Zhang generates the binding information at the head-end based on verification information from the POD and/or host (col. 4, lines 52-56), and the head end stores the verification information locally (col. 4, lines 54-55).

It is unclear what in Kim would correspond to the verification information upon which the CP signal is presumably based, or how this "on-the-fly" binding service (Zhang, col. 5, line 46) would avoid unacceptably slowing down decoding.

Based on the above, it would seem that Zhang, at best, might suggest:

a) that the stream, as augmented with the CP signal, is encrypted for transmission to the host, and

b) that this transmission is preceded by transmission, by the POD to the

host, of binding information such as "a private or secret key; a public key; a

predetermined signature; or other verification information" (col. 6, lines 4-5).

There is apparently no disclosure or suggestion in the references, alone or

in combination, of selecting, as the binding information, <u>payload</u> to be delivered across

the POD/host interface.

In addition, the Office Action suggests that it would have been obvious to

supply the Kim CP signal with a stream identifier, a proposition the applicant traverses.

Kim contemplates application to MPEG-2 streams (col. 2, line 8) which

have stream identifiers. Yet, Kim bears no hint of coupling the CP signal with a stream

identifier. This is just one more example of <u>impermissible hindsight</u> based on some

combination of the instant patent application and a reference that is <u>not</u> prior art, i.e., the

IS-POD-CP document mentioned above.

In particular, the combination of references the Office Action applies fails

to disclose, suggest or feature:

> point of deployment module generates a reply message which <u>includes at
> least one control information pair,</u> relating to the information, <u>each control
> information pair having copy control information</u> and a <u>stream identifier</u> . .
> . respectively <u>generating</u> a first key in the point of deployment module and
> a second key in the set-top box, <u>using the at least one control information
> pair</u>

which language appears explicitly in claim 1.

For at least the above reasons, it is unclear in what sense, and by what

motivation, the combination the Office Action proposes can properly be regarded as

featuring all the elements of claim 1. The combination is accordingly deemed not to

render obvious the present invention as recited in claim 1.

The Office Action cites, as motivation, providing "authentication of

devices as well as keeping data secure."

However, this motivation appears suited to the above-described best-

scenario embodiment, which does not meet the language of claim 1.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 2 recites, ". . . reply message from the deployment module to the

host device, wherein the reply message includes at least one control information pair,

each pair having a copy control information and a stream identifier. . . (c) generating a

first shared key at the host and a second shared key at the deployment module,

respectively, using the at least one control information pair. . ."

Claim 8 recites, ". . . the reply message including at least one control

information pair, each pair having copy control information and a stream identifier,

generating a first shared key using the at least one control information pair. . ."

Claim 13 recites, ". . . a reply message from the deployment module,

wherein the reply message includes at least one control information pair, each pair having

copy control information and a stream identifier, generating a second shared key using

the at least one control information pair. . ."

Claim 18 recites, ". . . a reply message to the host device, the reply

message including at least one control information pair, each pair having copy control

information and a stream identifier, generating a first shared key using the at least one

control information pair. . ."

Each of claims 2, 8, 13 and 18 are deemed to be patentable over the applied references for at least the reasons set forth above with regard to claim 1.

Claim 19 recites, ". . . wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least one control information pair, the respective copy control information of said at least one control information pair <u>not being encrypted</u> for the transmission."

The Office Action applies Zhang to Kim to introduce security concerns for transmission across the POD/host interface, and Zhang <u>encrypts</u> the binding information for transmission from the POD to the host (e.g., col. 8, line 56; col. 12, lines 30-31)

However, putting aside the inapplicability of the CP signal as set forth above, the Office Action suggests that the combination of references the Office Action cites moves the CP signal across the interface unencrypted.

Although the foregoing encryption might seem consistent with the language of claim 19, the applicant does not understand by what reasoning Kim/Zhang can be said to send the binding information across the POD/host interface unencrypted. Motivation cannot be gleaned from the instant patent application, at least because that would amount to impermissible hindsight.

The Office Action cites, as motivation, the idea that foregoing encryption of the binding information results in faster processing.

However, the application of Khang for security measures across the interface appears to suggest that the embodiment the Office Action proposes for claim 19 would not have been obvious.

<u>Reconsideration and withdrawal of the rejection is respectfully requested.</u>

Claim 20 recites, ". . . wherein step b) is executed without encrypting said

copy control information of said at least one control information pair."

Claim 21 recites, ". . . said copy control information of said at least one

control information pair in the reply message is unencrypted upon transmission to the

host device."

Each of claims 20 and 21 are deemed to be patentable over the applied

references for at least the reasons set forth above with regard to claim 19.

The Office Action first suggests that the stream ID shown in FIG. F.7 of

ITU-T serves as the "stream identifier" of claim 1, but this is incorrect.

The stream ID of FIG. F.7 identifies a type of elementary stream, and is

not uniquely identified with a particular elementary stream. Accordingly, the stream ID

does not uniquely identify a CCI assigned to a particular elementary stream.

The Office Action next suggests that a content identifier in an ECM

(entitlement control message) corresponds to the "stream identifier" of claim 1, but this is

incorrect. The ECM "content identifier," when present in an ECM, may identify a

category of the content. Although FIG. 21 in Kim shows an ECM and CPTC transmitted

by the smart card 261 to the controller 262, this does not suggest the coupling of a CCI

with an identifier of the particular elementary stream to which the CCI is assigned.

Incidentally, the suggestion by the Office Action that Kim uses the ECM

to identify the content appears to lack foundation, and does not appear to be supported by

the cited passage (lines 61-67 of column 18 in Kim).

For at least all of the above reasons, the cited combination of references

fails to render obvious the present invention as recited in claim 1.

As to independent claims 2, 8, 13 and 18, they are worded similarly to claim 1.

<u>Reconsideration and withdrawal of the rejections is respectfully requested.</u>

The remaining rejected claims each depend from one of the base claims and are likewise deemed non-obvious over the cited references for at least the same reason as that asserted for the respective base claim.

New claim 30 recites, ". . . the copy control information includes information on how many copies of an elementary stream can be made and on what copy formats are allowed." New claim 30 finds support in the specification (e.g., page 2, lines 23-29).
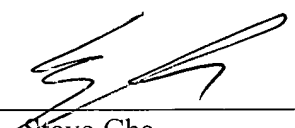
For all the foregoing reasons, it is respectfully submitted that all the present claims are patentable in view of the cited references. A Notice of Allowance is respectfully requested.

A check for $50.00 is enclosed in payment of the fee for adding one,

additional claim in excess of twenty total.

Respectfully submitted,

Dan Piotrowski
Registration No. 42,079

By: Steve Cha

Date: November 16, 2005

Attorney for Applicant
Registration No. 44,069

Mail all correspondence to:
Dan Piotrowski, Registration No. 42,079
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9624
Fax: (914) 332-0615